What is claimed is:

1. An elliptic curve arithmetic operation device for performing one of an addition and a doubling on an elliptic curve E: $y^2=f(x)$ on a residue class ring of polynomials in two variables α and β, moduli of the residue class ring being polynomials $\beta^2-f(\alpha)$ and $h(\alpha)$, where $f(\alpha)=\alpha^3+a\alpha+b$, a and b are constants, and $h(\alpha)$ is a polynomial in the variable α, the elliptic curve arithmetic operation device comprising:

acquiring means for acquiring affine coordinates of at least one point on the elliptic curve E and operation information indicating one of the addition and the doubling, from an external source;

transforming means for performing a coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates, the coordinate transformation being transforming affine coordinates $(\phi(\alpha), \beta\times\varphi(\alpha))$ of a given point on the elliptic curve E using polynomials

$$X(\alpha)=f(\alpha)\times\phi(\alpha)$$

$$Y(\alpha)=f(\alpha)^2\times\varphi(\alpha)$$

$$Z(\alpha)=1$$

into Jacobian coordinates $(X(\alpha):Y(\alpha):\beta\times Z(\alpha))$, $\phi(\alpha)$ and $\varphi(\alpha)$ being polynomials; and

operating means for performing one of the addition and the doubling indicated by the acquired operation information, on the

generated Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve *E*.

2. The elliptic curve arithmetic operation device of Claim 1,

wherein the acquiring means

(a) in a first case acquires affine coordinates of two different points on the elliptic curve *E* and operation information indicating the addition, and

(b) in a second case acquires affine coordinates of a single point on the elliptic curve *E* and operation information indicating the doubling,

wherein the transforming means

(a) in the first case performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates of the single point, and

wherein the operating means

(a) in the first case performs the addition indicated by the acquired operation information on the generated Jacobian coordinates of the two different points to obtain the Jacobian coordinates of the point on the elliptic curve *E*, and

(b) in the second case performs the doubling indicated by the acquired operation information on the generated Jacobian coordinates of the single point to obtain the Jacobian coordinates of the point on the elliptic curve *E*.

3. The elliptic curve arithmetic operation device of Claim 2,

wherein in the first case

the acquiring means acquires affine coordinates

$$(X1(\alpha), \beta\times Y1(\alpha))$$

$$(X2(\alpha), \beta\times Y2(\alpha))$$

of the two different points on the elliptic curve *E* and the operation information indicating the addition,

the transforming means performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta\times Z1(\alpha))$$

$$(X2(\alpha) : Y2(\alpha) : \beta\times Z2(\alpha))$$

of the two different points, and

the operating means computes

$$U1(\alpha)=X1(\alpha)\times Z2(\alpha)\ \hat{}\,2$$

$$U2(\alpha)=X2(\alpha)\times Z1(\alpha)\ \hat{}\,2$$

$$S1(\alpha)=Y1(\alpha)\times Z2(\alpha)\ \hat{}\,3$$

$$S2(\alpha)=Y2(\alpha)\times Z1(\alpha)\ \hat{}\,3$$

$$H(\alpha)=U2(\alpha)-U1(\alpha)$$

$$r(\alpha)=S2(\alpha)-S1(\alpha)$$

and computes

$$X3(\alpha)=-H(\alpha)\,\hat{}\,3-2\times U1(\alpha)\times H(\alpha)\,\hat{}\,2+r(\alpha)\,\hat{}\,2$$

$$Y3(\alpha)=-S1(\alpha)\times H(\alpha)\,\hat{}\,3+r(\alpha)\times(U1(\alpha)\times H(\alpha)\,\hat{}\,2-X3(\alpha))$$

$$Z3(\alpha)=Z1(\alpha)\times Z2(\alpha)\times H(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta\times Z3(\alpha))$ of the point on the elliptic curve E.

4. The elliptic curve arithmetic operation device of Claim 2,

wherein in the second case

the acquiring means acquires affine coordinates

$$(X1(\alpha),\beta\times Y1(\alpha))$$

of the single point on the elliptic curve E and the operation information indicating the doubling,

the transforming means performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates

$$(X1(\alpha):Y1(\alpha):\beta\times Z1(\alpha))$$

of the single point, and

the operating means computes

$$S(\alpha)=4\times X1(\alpha)\times Y1(\alpha)\,\hat{}\,2$$

$$M(\alpha)=3\times X1(\alpha)\,\hat{}\,2+a\times Z1(\alpha)\,\hat{}\,4\times f(\alpha)\,\hat{}\,2$$

$$T(\alpha)=-2\times S(\alpha)+M(\alpha)\hat{}2$$

and computes

$$X3(\alpha)=T(\alpha)$$

$$Y3(\alpha)=-8\times Y1(\alpha)\hat{}4+M(\alpha)\times(S(\alpha)-T(\alpha))$$

$$Z3(\alpha)=2\times Y1(\alpha)\times Z1(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta\times Z3(\alpha))$ of the point on the elliptic curve *E*.

5. The elliptic curve arithmetic operation device of Claim 2,

wherein the acquiring means

(a) in the first case acquires affine coordinates

$$(X1(\alpha),\beta\times Y1(\alpha))$$

$$(X2(\alpha),\beta\times Y2(\alpha))$$

of the two different points on the elliptic curve *E* and the operation information indicating the addition, and

(b) in the second case acquires affine coordinates

$$(X1(\alpha),\beta\times Y1(\alpha))$$

of the single point on the elliptic curve *E* and the operation information indicating the doubling,

wherein the transforming means

(a) in the first case performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates

$$(X1(\alpha):Y1(\alpha):\beta\times Z1(\alpha))$$

$$(X2(\alpha):Y2(\alpha):\beta\times Z2(\alpha))$$

of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates

$$(X1(\alpha):Y1(\alpha):\beta\times Z1(\alpha))$$

of the single point, and

wherein the operating means

(a) in the first case computes

$$U1(\alpha)=X1(\alpha)\times Z2(\alpha)\ \hat{}\,2$$

$$U2(\alpha)=X2(\alpha)\times Z1(\alpha)\ \hat{}\,2$$

$$S1(\alpha)=Y1(\alpha)\times Z2(\alpha)\ \hat{}\,3$$

$$S2(\alpha)=Y2(\alpha)\times Z1(\alpha)\ \hat{}\,3$$

$$H(\alpha)=U2(\alpha)-U1(\alpha)$$

$$r(\alpha)=S2(\alpha)-S1(\alpha)$$

and computes

$$X3(\alpha)=-H(\alpha)\ \hat{}\,3-2\times U1(\alpha)\times H(\alpha)\ \hat{}\,2+r(\alpha)\ \hat{}\,2$$

$$Y3(\alpha)=-S1(\alpha)\times H(\alpha)\ \hat{}\,3+r(\alpha)\times(U1(\alpha)\times H(\alpha)\ \hat{}\,2-X3(\alpha))$$

$$Z3(\alpha)=Z1(\alpha)\times Z2(\alpha)\times H(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta\times Z3(\alpha))$ of the point on the elliptic curve E, and

(b) in the second case computes

$$S(\alpha)=4\times X1(\alpha)\times Y1(\alpha)\ \hat{}\,2$$

$$M(\alpha)=3\times X1(\alpha)\hat{}2+a\times Z1(\alpha)\hat{}4\times f(\alpha)\hat{}2$$

$$T(\alpha)=-2\times S(\alpha)+M(\alpha)\hat{}2$$

and computes

$$X3(\alpha)=T(\alpha)$$

$$Y3(\alpha)=-8\times Y1(\alpha)\hat{}4+M(\alpha)\times(S(\alpha)-T(\alpha))$$

$$Z3(\alpha)=2\times Y1(\alpha)\times Z1(\alpha)$$

to obtain the Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta\times Z3(\alpha))$ of the point on the elliptic curve E.

6. An elliptic curve order computation device for computing an order of an elliptic curve according to a Schoof-Elkies-Atkin algorithm, comprising the elliptic curve arithmetic operation device of Claim 1.

7. The elliptic curve order computation device of Claim 6 comprising the elliptic curve arithmetic operation device of Claim 2.

8. The elliptic curve order computation device of Claim 7 comprising the elliptic curve arithmetic operation device of Claim 5.

9. An elliptic curve construction device for determining parameters of an elliptic curve E which is defined over a finite

field $GF(p)$ and offers a high level of security, p being a prime, the elliptic curve construction device comprising:

random number generating means for generating a random number;

parameter generating means for selecting the parameters of the elliptic curve E using the generated random number, in such a manner that a probability of a discriminant of the elliptic curve E having any square factor is lower than a predetermined threshold value;

finitude judging means for judging whether the elliptic curve E defined by the selected parameters has any point whose order is finite on a rational number field;

order computing means for computing an order m of the elliptic curve E when the finitude judging means judges that the elliptic curve E does not have any point whose order is finite on the rational number field;

security judging means for judging whether a condition that the computed order m is a prime not equal to the prime p is satisfied;

repeat controlling means for controlling the random number generating means, the parameter generating means, the finitude judging means, the order computing means, and the security judging means respectively to repeat random number generation, parameter selection, finitude judgement, order computation, and

security judgement until the condition is satisfied; and

parameter outputting means for outputting the selected parameters when the condition is satisfied.

10. The elliptic curve construction device of Claim 9,

wherein the elliptic curve *E* is expressed as $y^{\wedge}2=x^{\wedge}3+ax+b$, where parameters *a* and *b* are constants, and

wherein the parameter generating means selects *-3* and the random number respectively as the parameters *a* and *b* so that the probability of the discriminant of the elliptic curve *E* having any square factor is lower than the predetermined threshold value.

11. The elliptic curve construction device of Claim 10,

wherein the finitude judging means, given two primes *p1* and *p2* beforehand where $p1 \neq p2$, interprets the elliptic curve *E* as an elliptic curve *EQ* on the rational number field, computes orders *m1* and *m2* of respective elliptic curves *Ep1* and *Ep2* which are produced by reducing the elliptic curve *EQ* modulo *p1* and *p2*, judges whether the orders *m1* and *m2* are relatively prime, and, if the orders *m1* and *m2* are relatively prime, judges that the elliptic curve *E* does not have any point whose order is finite on the rational number field.

12. The elliptic curve construction device of Claim 11, wherein the finitude judging means, given the primes $p1=5$ and $p2=7$ beforehand, computes the orders $m1$ and $m2$ of the respective elliptic curves $Ep1$ and $Ep2$ produced by reducing the elliptic curve EQ modulo $p1=5$ and $p2=7$.

13. The elliptic curve construction device of Claim 11, wherein the order computing means computes the order m of the elliptic curve E according to a Schoof-Elkies-Atkin algorithm and includes

elliptic curve arithmetic operating means for performing one of an addition and a doubling on the elliptic curve $E: y^2=f(x)$ on a residue class ring of polynomials in variables α and β, moduli of the residue class ring being polynomials $\beta^2-f(\alpha)$ and $h(\alpha)$, where $f(\alpha)=\alpha^3+a\alpha+b$ and $h(\alpha)$ is a polynomial in the variable α,

wherein the elliptic curve arithmetic operating means includes the elliptic curve arithmetic operation device of Claim 1.

14. The elliptic curve construction device of Claim 13, wherein the elliptic curve arithmetic operating means includes the elliptic curve arithmetic operation device of Claim 2.

15. The elliptic curve construction device of Claim 14, wherein the elliptic curve arithmetic operating means includes the elliptic curve arithmetic operation device of Claim 5.

16. An elliptic curve application device that uses elliptic curves, comprising

elliptic curve constructing means for determining parameters of an elliptic curve *E* which is defined over a finite field *GF(p)* and offers a high level of security, *p* being a prime,

wherein the elliptic curve constructing means includes the elliptic curve construction device of Claim 9.

17. The elliptic curve application device of Claim 16, wherein the elliptic curve constructing means includes the elliptic curve construction device of Claim 10.

18. The elliptic curve application device of Claim 17, wherein the elliptic curve constructing means includes the elliptic curve construction device of Claim 11.

19. The elliptic curve application device of Claim 18, wherein the elliptic curve constructing means includes the

elliptic curve construction device of Claim 12.

20. The elliptic curve application device of Claim 18, wherein the elliptic curve constructing means includes the elliptic curve construction device of Claim 13.

21. The elliptic curve application device of Claim 20, wherein the elliptic curve constructing means includes the elliptic curve construction device of Claim 14.

22. The elliptic curve application device of Claim 21, wherein the elliptic curve constructing means includes the elliptic curve construction device of Claim 15.

23. An elliptic curve arithmetic operation method used in an elliptic curve arithmetic operation device equipped with an acquiring means, a transforming means, and an operating means, for performing one of an addition and a doubling on an elliptic curve $E: y^2=f(x)$ on a residue class ring of polynomials in two variables α and β, moduli of the residue class ring being polynomials $\beta^2-f(\alpha)$ and $h(\alpha)$, where $f(\alpha)=\alpha^3+a\alpha+b$, a and b are constants, and $h(\alpha)$ is a polynomial in the variable α, the elliptic curve arithmetic operation method comprising:

an acquiring step performed by the acquiring means, for

acquiring affine coordinates of at least one point on the elliptic curve E and operation information indicating one of the addition and the doubling, from an external source;

a transforming step performed by the transforming means, for performing a coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates, the coordinate transformation being transforming affine coordinates $(\phi(\alpha), \beta\times\varphi(\alpha))$ of a given point on the elliptic curve E using polynomials

$$X(\alpha)=f(\alpha)\times\phi(\alpha)$$

$$Y(\alpha)=f(\alpha)\hat{}2\times\varphi(\alpha)$$

$$Z(\alpha)=1$$

into Jacobian coordinates $(X(\alpha):Y(\alpha):\beta\times Z(\alpha))$, $\phi(\alpha)$ and $\varphi(\alpha)$ being polynomials; and

an operating step performed by the operating means, for performing one of the addition and the doubling indicated by the acquired operation information, on the generated Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve E.

24. An elliptic curve construction method used in an elliptic curve construction device equipped with random number generating means, parameter generating means, finitude judging means, order computing means, security judging means, repeat controlling means, and parameter outputting means, for determining parameters

of an elliptic curve *E* which is defined over a finite field *GF(p)* and offers a high level of security, *p* being a prime, the elliptic curve construction method comprising:

a random number generating step performed by the random number generating means, for generating a random number;

a parameter generating step performed by the parameter generating means, for selecting the parameters of the elliptic curve *E* using the generated random number, in such a manner that a probability of a discriminant of the elliptic curve *E* having any square factor is lower than a predetermined threshold value;

a finitude judging step performed by the finitude judging means, for judging whether the elliptic curve *E* defined by the selected parameters has any point whose order is finite on a rational number field;

an order computing step performed by the order computing means, for computing an order *m* of the elliptic curve *E* when the finitude judging step judges that the elliptic curve *E* does not have any point whose order is finite on the rational number field;

a security judging step performed by the security judging means, for judging whether a condition that the computed order *m* is a prime not equal to the prime *p* is satisfied;

a repeat controlling step performed by the repeat controlling

means, for controlling the random number generating step, the parameter generating step, the finitude judging step, the order computing step, and the security judging step respectively to repeat random number generation, parameter selection, finitude judgement, order computation, and security judgement until the condition is satisfied; and

a parameter outputting step performed by the parameter outputting means, for outputting the selected parameters when the condition is satisfied.

25. A computer-readable storage medium storing an elliptic curve arithmetic operation program used in an elliptic curve arithmetic operation device equipped with acquiring means, transforming means, and operating means, for performing one of an addition and a doubling on an elliptic curve $E: y^2=f(x)$ on a residue class ring of polynomials in two variables α and β, moduli of the residue class ring being polynomials $\beta^2-f(\alpha)$ and $h(\alpha)$, where $f(\alpha)=\alpha^3+a\alpha+b$, a and b are constants, and $h(\alpha)$ is a polynomial in the variable α, the elliptic curve arithmetic operation program comprising:

an acquiring step performed by the acquiring means, for acquiring affine coordinates of at least one point on the elliptic curve E and operation information indicating one of the addition and the doubling, from an external source;

a transforming step performed by the transforming means, for performing a coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates, the coordinate transformation being transforming affine coordinates $(\phi(\alpha),\beta\times\varphi(\alpha))$ of a given point on the elliptic curve E using polynomials

$$X(\alpha)=f(\alpha)\times\phi(\alpha)$$

$$Y(\alpha)=f(\alpha)\hat{}2\times\varphi(\alpha)$$

$$Z(\alpha)=1$$

into Jacobian coordinates $(X(\alpha):Y(\alpha):\beta\times Z(\alpha))$, $\phi(\alpha)$ and $\varphi(\alpha)$ being polynomials; and

an operating step performed by the operating means, for performing one of the addition and the doubling indicated by the acquired operation information, on the generated Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve E.

26. The storage medium of Claim 25,

wherein the acquiring step

(a) in a first case acquires affine coordinates of two different points on the elliptic curve E and operation information indicating the addition, and

(b) in a second case acquires affine coordinates of a single point on the elliptic curve E and operation information indicating the doubling,

wherein the transforming step

(a) in the first case performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates of the single point, and

wherein the operating step

(a) in the first case performs the addition indicated by the acquired operation information on the generated Jacobian coordinates of the two different points to obtain the Jacobian coordinates of the point on the elliptic curve *E*, and

(b) in the second case performs the doubling indicated by the acquired operation information on the generated Jacobian coordinates of the single point to obtain the Jacobian coordinates of the point on the elliptic curve *E*.

27. The storage medium of Claim 26,

wherein in the first case

the acquiring step acquires affine coordinates

$$(X1(\alpha), \beta \times Y1(\alpha))$$

$$(X2(\alpha), \beta \times Y2(\alpha))$$

of the two different points on the elliptic curve *E* and the operation information indicating the addition,

the transforming step performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates

$$(X1(\alpha):Y1(\alpha):\beta\times Z1(\alpha))$$

$$(X2(\alpha):Y2(\alpha):\beta\times Z2(\alpha))$$

of the two different points, and

the operating step computes

$$U1(\alpha)=X1(\alpha)\times Z2(\alpha)^{2}$$

$$U2(\alpha)=X2(\alpha)\times Z1(\alpha)^{2}$$

$$S1(\alpha)=Y1(\alpha)\times Z2(\alpha)^{3}$$

$$S2(\alpha)=Y2(\alpha)\times Z1(\alpha)^{3}$$

$$H(\alpha)=U2(\alpha)-U1(\alpha)$$

$$r(\alpha)=S2(\alpha)-S1(\alpha)$$

and computes

$$X3(\alpha)=-H(\alpha)^{3}-2\times U1(\alpha)\times H(\alpha)^{2}+r(\alpha)^{2}$$

$$Y3(\alpha)=-S1(\alpha)\times H(\alpha)^{3}+r(\alpha)\times(U1(\alpha)\times H(\alpha)^{2}-X3(\alpha))$$

$$Z3(\alpha)=Z1(\alpha)\times Z2(\alpha)\times H(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta\times Z3(\alpha))$ of the point on the elliptic curve E.

28. The storage medium of Claim 26,

wherein in the second case

the acquiring step acquires affine coordinates

$$(X1(\alpha),\beta\times Y1(\alpha))$$

of the single point on the elliptic curve E and the operation information indicating the doubling,

the transforming step performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates

$$(X1(\alpha):Y1(\alpha):\beta\times Z1(\alpha))$$

of the single point, and

the operating step computes

$$S(\alpha)=4\times X1(\alpha)\times Y1(\alpha)^{2}$$

$$M(\alpha)=3\times X1(\alpha)^{2}+a\times Z1(\alpha)^{4}\times f(\alpha)^{2}$$

$$T(\alpha)=-2\times S(\alpha)+M(\alpha)^{2}$$

and computes

$$X3(\alpha)=T(\alpha)$$

$$Y3(\alpha)=-8\times Y1(\alpha)^{4}+M(\alpha)\times(S(\alpha)-T(\alpha))$$

$$Z3(\alpha)=2\times Y1(\alpha)\times Z1(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta\times Z3(\alpha))$ of the point on the elliptic curve E.

29. The storage medium of Claim 26,

wherein the acquiring step

(a) in the first case acquires affine coordinates

$$(X1(\alpha),\beta\times Y1(\alpha))$$

$$(X2(\alpha),\beta\times Y2(\alpha))$$

of the two different points on the elliptic curve E and the

operation information indicating the addition, and

(b) in the second case acquires affine coordinates

$$(X1(\alpha), \beta\times Y1(\alpha))$$

of the single point on the elliptic curve *E* and the operation information indicating the doubling,

wherein the transforming step

(a) in the first case performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta\times Z1(\alpha))$$

$$(X2(\alpha) : Y2(\alpha) : \beta\times Z2(\alpha))$$

of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta\times Z1(\alpha))$$

of the single point, and

wherein the operating step

(a) in the first case computes

$$U1(\alpha)=X1(\alpha)\times Z2(\alpha)\,{}^{\wedge}2$$

$$U2(\alpha)=X2(\alpha)\times Z1(\alpha)\,{}^{\wedge}2$$

$$S1(\alpha)=Y1(\alpha)\times Z2(\alpha)\,{}^{\wedge}3$$

$$S2(\alpha)=Y2(\alpha)\times Z1(\alpha)\,{}^{\wedge}3$$

$$H(\alpha)=U2(\alpha)-U1(\alpha)$$

$$r(\alpha)=S2(\alpha)-S1(\alpha)$$

and computes

$$X3(\alpha)=-H(\alpha)^3-2\times U1(\alpha)\times H(\alpha)^2+r(\alpha)^2$$

$$Y3(\alpha)=-S1(\alpha)\times H(\alpha)^3+r(\alpha)\times(U1(\alpha)\times H(\alpha)^2-X3(\alpha))$$

$$Z3(\alpha)=Z1(\alpha)\times Z2(\alpha)\times H(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta\times Z3(\alpha))$ of the point on the elliptic curve E, and

(b) in the second case computes

$$S(\alpha)=4\times X1(\alpha)\times Y1(\alpha)^2$$

$$M(\alpha)=3\times X1(\alpha)^2+a\times Z1(\alpha)^4\times f(\alpha)^2$$

$$T(\alpha)=-2\times S(\alpha)+M(\alpha)^2$$

and computes

$$X3(\alpha)=T(\alpha)$$

$$Y3(\alpha)=-8\times Y1(\alpha)^4+M(\alpha)\times(S(\alpha)-T(\alpha))$$

$$Z3(\alpha)=2\times Y1(\alpha)\times Z1(\alpha)$$

to obtain the Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta\times Z3(\alpha))$ of the point on the elliptic curve E.

30. A computer-readable storage medium storing an elliptic curve construction program used in an elliptic curve construction device equipped with random number generating means, parameter generating means, finitude judging means, order computing means, security judging means, repeat controlling means, and parameter outputting means, for determining parameters of an elliptic curve

E which is defined over a finite field *GF(p)* and offers a high level of security, *p* being a prime, the elliptic curve construction program comprising:

a random number generating step performed by the random number generating means, for generating a random number;

a parameter generating step performed by the parameter generating means, for selecting the parameters of the elliptic curve *E* using the generated random number, in such a manner that a probability of a discriminant of the elliptic curve *E* having any square factor is lower than a predetermined threshold value;

a finitude judging step performed by the finitude judging means, for judging whether the elliptic curve *E* defined by the selected parameters has any point whose order is finite on a rational number field;

an order computing step performed by the order computing means, for computing an order *m* of the elliptic curve *E* when the finitude judging step judges that the elliptic curve *E* does not have any point whose order is finite on the rational number field;

a security judging step performed by the security judging means, for judging whether a condition that the computed order *m* is a prime not equal to the prime *p* is satisfied;

a repeat controlling step performed by the repeat controlling

means, for controlling the random number generating step, the parameter generating step, the finitude judging step, the order computing step, and the security judging step respectively to repeat random number generation, parameter selection, finitude judgement, order computation, and security judgement until the condition is satisfied; and

a parameter outputting step performed by the parameter outputting means, for outputting the selected parameters when the condition is satisfied.

31. The storage medium of Claim 30,

wherein the elliptic curve E is expressed as $y\hat{\ }2=x\hat{\ }3+ax+b$, where parameters a and b are constants, and

wherein the parameter generating step selects -3 and the random number respectively as the parameters a and b so that the probability of the discriminant of the elliptic curve E having any square factor is lower than the a predetermined threshold value.

32. The storage medium of Claim 31,

wherein the finitude judging step, given two primes $p1$ and $p2$ beforehand where $p1 \neq p2$, interprets the elliptic curve E as an elliptic curve EQ on the rational number field, computes orders $m1$ and $m2$ of respective elliptic curves $Ep1$ and $Ep2$ which are

produced by reducing the elliptic curve EQ modulo $p1$ and $p2$, judges whether the orders $m1$ and $m2$ are relatively prime, and, if the orders $m1$ and $m2$ are relatively prime, judges that the elliptic curve E does not have any point whose order is finite on the rational number field.

33. The storage medium of Claim 32,

wherein the finitude judging step, given the primes $p1=5$ and $p2=7$ beforehand, computes the orders $m1$ and $m2$ of the respective elliptic curves $Ep1$ and $Ep2$ produced by reducing the elliptic curve EQ modulo $p1=5$ and $p2=7$.